Welcome to the PIA for FY 2010!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate “personally identifiable information” of the public. Personally identifiable information, or “personal information,” is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program. More information can be found by reading VA 6508.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: http://vaww.privacy.va.gov/Privacy_Impact_Assessments.asp

Roles and Responsibilities:

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the Privacy Impact Assessment Handbook 6202.2 referenced in the procedure section of this document.

a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Handbook 6202.2.

b. Records Officer is responsible for supplying records retention and deletion schedules.

c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Handbook 6202.2 and to immediately report all anomalies to the Privacy Service and appropriate management chain.

d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.

e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and systems, coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues, and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)

Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect indentify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form

To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

(FY 2010) PIA: System Identification

Program or System Name: Region 3 > VHA > VISN 9> Huntington VAMC > VISTA-VMS

OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-01-11-01-1180-0

Description of System / Application / Program: The VISTA system is designed to operate as a fully integrated clinical and administrative information source. It processes clinical information, information covered by the Privacy Act & HIPAA, PHI/ePHI, financial records, and all other data necessary to run a tertiary medical center. All clinical and most administrative functions within the physical confines of the VISN9 utilize the VISTA Alpha cluster to process clinical, financial, or administrative data. All external organizations which access a local Alpha node must be authenticated by access and verify codes or by domain transmission scripts for electronic mail. Examples of these organizations include VBA Regional Office, Form, HINQ, all VA facilities throughout the country sending electronic mail, Medical Cost Recovery vendors and transcription vendors. The native operating system of the Alpha cluster is VMS. Cache is a programming language that runs on top of VMS. Using the Cache environment, the VA's VISTA program exists with all attendant menus, parameters, and data. Cache is the only application inhabiting the Alpha cluster.

Facility Name: Huntington VAMC

Title:	Name:	Phone:	Email:
Privacy Officer:	Diana Bowen	304-429-6755 e	diana.bowen@va.gov
Information Security Officer:	Vickie Hisman	304-429-6755 e	vickie.hisman@va.gov
Chief Information Officer:	Mary Curry	304-429-6755 e	mary.curry@va.gov
Person Completing Document:	Vickie Hisman		
Other Titles:			

Other Titles:

Other Titles:

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY) 07/2009

Date Approval To Operate Expires: 08/2011

What specific legal authorities authorize this program or system:	Title 38, United States Code, section 7301(a).
What is the expected number of individuals that will have their PII stored in this system:	125,000-150,000
Identify what stage the System / Application / Program is at:	Operation/Maintenance
The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.	Approximately 27 years
Is there an authorized change control process which documents any changes to existing applications or systems?	Yes
If No, please explain:	
Has a PIA been completed within the last three years?	Yes
Date of Report (MM/YYYY):	07/2008

Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.

☑ Have any changes been made to the system since the last PIA?

☑ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?

☑ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?

☑ Does this system/application/program collect, store or disseminate PII/PHI data?

☑ Does this system/application/program collect, store or disseminate the SSN?

If there is no Personally Identifiable Information on your system , please skip to TAB 12. (See Comment for Definition of PII)

(FY 2010) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? if the answer above is no, please skip to row 16.	Yes
For each applicable System(s) of Records, list:	
1. All System of Record Identifier(s) (number):	97VA105
2. Name of the System of Records:	Consolidated Data Information System-VA
3. Location where the specific applicable System of Records Notice may be accessed (include the URL):	http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm
Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?	Yes
Does the System of Records Notice require modification or updating?	No
	(Please Select Yes/No)
Is PII collected by paper methods?	Yes
Is PII collected by verbal methods?	Yes
Is PII collected by automated methods?	Yes
Is a Privacy notice provided?	Yes
Proximity and Timing: Is the privacy notice provided at the time of data collection?	Yes
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	Yes
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	Yes
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	Yes

(FY 2010) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	ALL	That the information will be used to enter them in the computer and will be used for future identification, correspondence & contact	Verbal & Written	Written
Family Relation (spouse, children, parents, grandparents, etc)	ALL	We ask for this information in case we need to contact the next of kin; also, information is taken regarding household	Verbal & Written	Written
Service Information	ALL	For benefits	Verbal & Written	Written
Medical Information	Verbal	For diagnostic & treatment purposes	Verbal & Written	Written
Criminal Record Information	Electronic/File Transfer	Used if there is a criminal investigation that the individual is involved in.	Verbally	Written
Guardian Information	Verbal	For decision making	Verbally	Written
Education Information	ALL	For employment purposes	All	Written
Benefit Information	ALL	To determine eligibility for treament/benefits	Verbal & Written	Written
Other (Explain)				

Data Type	Is Data Type Stored on your system?	**Source** (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Mandatory	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Mandatory	
Service Information				HINQ, HEC, Veterans' Information Solution, Regional Office, St. Louis

Medical Information	Yes	Veteran	Mandatory	
Criminal Record Information	Yes	State Agency (Identify)	Mandatory	WV Automated Police Network
Guardian Information	Yes	Veteran	Voluntary	
Education Information	Yes	VA Files / Databases (Identify file)	Mandatory	USAJOBS.gov
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory	HINQ, HEQ, Veterans' Information Solution, St. Louis National Archives
Other (Explain)				
Other (Explain)				
Other (Explain)				

(FY 2010) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	Regional Counsel	No	Veterans Health Records reviewed for Tort Claims, legal processes.	Both PII & PHI	VHA 1605.1 and VHA 1605.2 Handbooks, MCM MR8
Other Veteran Organization	VBA/Regional Office	Yes	Veterans Health Records of treatment and demographic records for benefits determination.	Both PII & PHI	VHA 1605.1 and VHA 1605.2 Handbooks, MCM MR8
Other Federal Government Agency	1) Social Security Administration 2) Enquiries by Congress 3) Center for Disease Control	No	1) Medical information for claims; benefit information for eligibility 2) Information requested on behalf of the patient; it could be anything in our records that the patient authorizes their Congressional representative to have.	Both PII & PHI	VHA 1605.1 and VHA 1605.2 Handbooks, MCM MR8
State Government Agency	WV Department of Health & Human Services	No	Communicable Disease Reporting as well as certain injuries (GSWs, etc) to help ensure community health	Both PII & PHI	VHA 1605.1 and VHA 1605.2 Handbooks, MCM MR8
Local Government Agency	County Coroner's Office	No	Date of Death, circumstances & death certificate	Both PII & PHI	VHA 1605.1 and VHA 1605.2 Handbooks, MCM MR8
Research Entity	Facility employees who are involved in research projects	Yes	Medical info is shared for research purposes	Both PII & PHI	VHA 1605.1 and VHA 1605.2 Handbooks, MCM MR8

Other Project / System	Multiple Contractors with VPN Access: 1) Allied Interstate 2) WV Veterans' Home 3) Tri State Cancer 4) MedScripts 5) MCCR AR 6) Health Management Systems 7) Preferred Medical 8) Mountaineer Imaging	Yes	1) Medical information for billing insurance claims 2) View only access to medical information of our patients who reside there 3) Medical information for treatment 4) Transcription services for medical reports 5) Medical information for billing insurance 6) Medical information for billing insurance claims 7) Medical information for billing insurance claims 8) Contract radiologist who views images & provides reports	Both PII & PHI	VHA 1605.1 and VHA 1605.2 Handbooks, MCM MR8
Other Project / System					
Other Project / System					

(FY 2010) PIA: Access to Records

Does the system gather information from another system?	Yes
Please enter the name of the system:	Medscripts Transcription, VBA, Healthy Buddy
Per responses in Tab 4, does the system gather information from an individual?	Yes
If information is gathered from an individual, is the information provided:	☑ Through a Written Request ☑ Submitted in Person ☑ Online via Electronic Form
Is there a contingency plan in place to process information when the system is down?	Yes

(FY 2010) PIA: Secondary Use

Will PII data be included with any secondary use request?	Yes
if yes, please check all that apply:	☑ Drug/Alcohol Counseling ☑ Mental Health ☑ HIV ☑ Research ☑ Sickle Cell ☑ Other (Please Explain)
Describe process for authorizing access to this data. Answer:	Research Research application is approved by the IRB and then PII information is accessed with consent for Research protocols but de-identified in Research documents. 7332 diagnoses must have consent from the patient or their representative. On non 7332 diagnoses, if there is no consent from the patient, then a HIPAA waiver must be approved by the IRB.

(FY 2010) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?	No
If Yes, Please Specify:	

Explain how collected data are limited to required elements:

Answer: The software limits the amount/type of data that is collected. Data is collected electronically and elements selected based on the automation of VA Forms and clinical procedures. Forms are designed to collect only necessary data. Electronic data transfers are subject to design criteria, industry format standards and automated checks to ensure that only appropriate data is contained in the transfer. The web sites' privacy statements
(http://www.va.gov/privacy/index.htm) certify that personally identifying information provided by the veteran will be used only in connection with VA programs and services or for such purposes as are described at the point of collection. Scanning is usually limited to documents that are sent from non-VA providers to maintain a complete medical record. Information is not usually
gathered over the phone. If it is, it is minimal information used to fill in a pre-approved form

How is data checked for completeness?

Answer: Many software applications check to see if necessary data is entered, otherwise information that is entered is compared to the answers given by the patient. Audits are performed by the responsible department to ensure the information is complete.
Hard Copy: The department responsible for that form checks to make sure all necessary information is included.
WebSite: Software applications check to see if necessary data is entered.
Phone: Based on completing a hard copy so department responsible for that form checks to make sure all necessary information is included.
Scanning: Documents received from outside providers are scanned into the record. Clerk may contact outside provider if document seems incomplete.

What steps or procedures are taken to ensure the data remains current and not out of date?

Answer: Patients are required to update their administrative information at least twice yearly. Reminders are set for the staff. Medical information is as current as their most recent visit. Medical Center
staff receive a electronic reminder when opening the patient's record if the patient info needs to be updated. The staff then tells the patient that they need to report to the eligibility office.
Reminders are also mailed to the patient

How is new data verified for relevance, authenticity and accuracy?

Answer: The patient is required to provide updated information upon registration for each encounter. If there is a significant change in the data, the registrar repeats the question to assure accuracy.

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer: None

(FY 2010) PIA: Retention & Disposal

What is the data retention period?

Answer: Clinical information is retained in accordance with VA Records Control Schedule 10-1. Demographic information is updated as applications for care are submitted and retained in accordance with VA RCS 10-1. Records are retained to assure continuity of care, provider reference and patient reference as needed and deemed appropriate. All medical documents are maintained for 75 years.

Explain why the information is needed for the indicated retention period?

Answer: Healthcare & research.

What are the procedures for eliminating data at the end of the retention period?

Answer: Electronic Final Version of Patient Medical Record is destroyed/deleted 75 years after the last episode of patient care as instructed in VA RCS 10-1. Paper documents are maintained in retirement for 75 years following episode of care.

Where are these procedures documented?

Answer: VA Handbook 6300; RCS 10-1

How are data retention procedures enforced?

Answer: VA RCS 10-1 (page 8). The Health Information Resource Service (HIRS) is responsible for developing policies and procedures for effective and efficient records management throughout VHA. In addition, HIRS acts as the liaison between VHA and National Archives and Records Administration (NARA) on issues pertaining to records management practices & procedures. Following VHA policy, the Director or his/her designee is responsible for enforcing the policy on retention and destruction.

Has the retention schedule been approved by the National Archives and Records Administration (NARA)	Yes

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer: None

(FY 2010) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13?	No

If Yes, How will parental or guardian approval be obtained?

Answer:

(FY 2010) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.	Yes
Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..	Yes
Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes

If 'No' to any of the 3 questions above, please describe why:
Answer:

Is adequate physical security in place to protect against unauthorized access?	Yes

If 'No' please describe why:
Answer: POA&MS with projects in place to correct identified deficiency

Explain how the project meets IT security requirements and procedures required by federal law.
Answer: Continuous monitoring of POAMs & ongoing audits, annual FISMA assessment; C&A, ITOC inspections; The Certification & Accreditation (C&A) of the VISTA system is continuous. Huntington's VISTA system received full authority to operate in 2008 via the C&A process. The Information Security Officer continuously monitors all security controls at OI&T defined intervals. Assessment is completed in SMART database, Continuous monitoring documentation is also done through SMART. Tools used for Field monitoring include STAT Guardian, EPO Console, Sanctuary, Event Viewer, SMS Web Reports, and NetIQ Vulnerability Manager Reports. The facility periodically reviews/updates System Security Plans that addresses required security control policy and procedures consistent with applicable laws and guidance.

Explain what security risks were identified in the security assessment? *(Check all that apply)*

☑ Air Conditioning Failure
☑ Chemical/Biological Contamination
☑ Blackmail
☑ Bomb Threats
☑ Cold/Frost/Snow
☑ Communications Loss
☑ Computer Intrusion
☑ Data Destruction
☑ Data Disclosure
☑ Data Integrity Loss
☑ Denial of Service Attacks
□ Earthquakes
☑ Eavesdropping/Interception
☑ Fire (False Alarm, Major, and Minor)
☑ Flooding/Water Damage

☑ Hardware Failure
☑ Malicious Code
☑ Computer Misuse
☑ Power Loss
☑ Sabotage/Terrorism
☑ Storms/Hurricanes
□ Substance Abuse
☑ Theft of Assets
☑ Theft of Data
☑ Vandalism/Rioting
☑ Errors (Configuration and Data Entry)
☑ Burglary/Break In/Robbery
☑ Identity Theft
☑ Fraud/Embezzlement

Answer: (Other Risks)

Explain what security controls are being used to mitigate these risks. *(Check all that apply)*

☑ Risk Management
☑ Access Control
☑ Awareness and Training
☑ Contingency Planning
☑ Physical and Environmental Protection
☑ Personnel Security
☑ Certification and Accreditation Security Assessments

☑ Audit and Accountability
☑ Configuration Management
☑ Identification and Authentication
☑ Incident Response
☑ Media Protection

Answer: (Other Controls) N/A

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

Answer: Eliminate unnecessary collection of PII and ensure access controls are enforced

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☑ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals. □ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals. □ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☑ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals. □ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals. □ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization? **(Choose One)**	☑ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals. □ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals. □ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
The controls are being considered for the project based on the selections from the previous assessments?	Yes

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

Please add additional controls:

(FY 2010) PIA: Additional Comments

Add any additional comments on this tab for any question in the form you want to comment on.
Please indicate the question you are responding to and then add your comments.

Explain what minor application that are associated with your installation? *(Check all that apply)*

Records Locator System
Veterans Assistance Discharge System (VADS)
LGY Processing
Loan Service and Claims
LGY Home Loans
Search Participant Profile (SPP)
Control of Veterans Records (COVERS)
SHARE
Modern Awards Process Development (MAP-D)
Rating Board Automation 2000 (RBA2000)
State of Case/Supplemental (SOC/SSOC)
Awards
Financial and Accounting System (FAS)
Eligibility Verification Report (EVR)
Automated Medical Information System (AMIS)290
Web Automated Reference Material System (WARMS)
Automated Standardized Performace Elements Nationwide (ASPEN)
Inquiry Routing Information System (IRIS)
National Silent Monitoring (NSM)
Web Service Medical Records (WebSMR)
Systematic Technical Accuracy Review (STAR)
Fiduciary STAR Case Review
Veterans Exam Request Info System (VERIS)
Web Automated Folder Processing System (WAFPS)
Courseware Delivery System (CDS)
Electronic Performance Support System (EPSS)
Veterans Service Representative (VSR) Advisor
Loan Guaranty Training Website
C&P Training Website

Education Training Website
VR&E Training Website
VA Reserve Educational Assistance Program
Web Automated Verification of Enrollment
Right Now Web
VA Online Certification of Enrollment (VA-ONCE
Automated Folder Processing System (AFPS)
Personal Computer Generated Letters (PCGL)
Personnel Information Exchange System (PIES)
Rating Board Automation 2000 (RBA2000)
SHARE
State Benefits Reference System
Training and Performance Support System (TPSS)
Veterans Appeals Control and Locator System (VACOLS)
Veterans On-Line Applications (VONAPP)
Automated Medical Information Exchange II (AIME II)
Committee on Waivers and Compromises (COWC)
Common Security User Manager (CSUM)
Compensation and Pension (C&P) Record Interchange (CAPRI)
Control of Veterans Records (COVERS)
Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
Fiduciary Beneficiary System (FBS)
Hearing Officer Letters and Reports System (HOLAR)
Inforce
Awards
Actuarial
Insurance Self Service
Insurance Unclaimed Liabilities
Insurance Online

Appraisal System
Web Electronic Lender Identification
CONDO PUD Builder
Centralized Property Tracking System
Electronic Appraisal System
Web LGY
Access Manager
SAHSHA
VBA Data Warehouse
Distribution of Operational Resources (DOOR)
Enterprise Wireless Messaging System (Blackberry)
VBA Enterprise Messaging System
LGY Centralized Fax System
Review of Quality (ROQ)
Automated Sales Reporting (ASR)
Electronic Card System (ECS)
Electronic Payroll Deduction (EPD)
Financial Management Information System (FMI)
Purchase Order Management System (POMS)
Veterans Canteen Web
Inventory Management System (IMS)
Synquest
RAI/MDS
ASSISTS
MUSE
Bbraun (CP Hemo)
VIC
BCMA Contingency Machines
Script Pro

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Minor app #1

Name	Description	Comments

□ Is PII collected by this min or application?

□ Does this minor application store PII?

If yes, where?

Who has access to this data?

Minor app #2

Name	Description	Comments

□ Is PII collected by this min or application?

□ Does this minor application store PII?

If yes, where?

Who has access to this data?

Minor app #3

Name	Description	Comments

□ Is PII collected by this min or application?

□ Does this minor application store PII?

If yes, where?

Who has access to this data?

Baker System

Dental Records Manager

Sidexis

Priv Plus

Mental Health Asisstant

Telecare Record Manager

Omnicell

Powerscribe Dictation System

EndoSoft

Compensation and Pension (C&P)

Montgomery GI Bill

Vocational Rehabilitation & Employment (VR&E) CH 31

Post Vietnam Era educational Program (VEAP) CH 32

Spinal Bifida Program Ch 18

C&P Payment System

Survivors and Dependents Education Assistance CH 35

Reinstatement Entitelment Program for Survivors (REAPS)

Educational Assistance for Members of the Selected Reserve Program CH 1606

Reserve Educational Assistance Program CH 1607

Compensation & Pension Training Website

Web-Enabled Approval Management System (WEAMS)

FOCAS

Work Study Management System (WSMS)

Benefits Delivery Network (BDN)

Personnel and Accounting Integrated Data and Fee Basis (PAID)

Personnel Information Exchange System (PIES)

Rating Board Automation 2000 (RBA2000)

SHARE

Service Member Records Tracking System

Veterans Assistance Discharge System (VADS)

VBA Training Academy

Veterans Service Network (VETSNET)

Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)

BIRLS

Centralized Accounts Receivable System (CARS)

Compensation & Pension (C&P)

Corporate Database

Control of Veterans Records (COVERS)

Data Warehouse

INS - BIRLS

Mobilization

Master Veterans Record (MVR

BDN Payment History

(FY 2010) PIA: VISTA Minor Applications

Explain what minor application that are associated with your installation? *(Check all that apply)*

x	ACCOUNTS RECEIVABLE	x	DRUG ACCOUNTABILITY	x	INPATIENT MEDICATIONS	x
	ADP PLANNING (PLANMAN)	x	DSS EXTRACTS	x	INTAKE/OUTPUT	x
x	ADVERSE REACTION TRACKING		EDUCATION TRACKING	x	INTEGRATED BILLING	x
X	ASISTS		EEO COMPLAINT TRACKING	x	INTEGRATED PATIENT FUNDS	x
x	AUTHORIZATION/SUBSCRIPTION	x	ELECTRONIC SIGNATURE		INTERIM MANAGEMENT SUPPORT	
x	AUTO REPLENISHMENT/WARD STOCK	x	ENGINEERING	x	KERNEL	x
x	AUTOMATED INFO COLLECTION SYS	x	ENROLLMENT APPLICATION SYSTEM	x	KIDS	x
x	AUTOMATED LAB INSTRUMENTS	x	EQUIPMENT/TURN-IN REQUEST	x	LAB SERVICE	
x	AUTOMATED MED INFO EXCHANGE	x	EVENT CAPTURE		LETTERMAN	x
x	BAR CODE MED ADMIN		EVENT DRIVEN REPORTING	x	LEXICON UTILITY	x
X	BED CONTROL		EXTENSIBLE EDITOR	x	LIBRARY	
X	BENEFICIARY TRAVEL	x	EXTERNAL PEER REVIEW	x	LIST MANAGER	x
	CAPACITY MANAGEMENT - RUM	x	FEE BASIS	x	MAILMAN	x
X	CAPRI	x	FUNCTIONAL INDEPENDENCE	x	MASTER PATIENT INDEX VISTA	x
x	CAPACITY MANAGEMENT TOOLS		GEN. MED. REC. - GENERATOR		MCCR NATIONAL DATABASE	x
x	CARE MANAGEMENT		GEN. MED. REC. - I/O	x	MEDICINE	x
x	CLINICAL CASE REGISTRIES	x	GEN. MED. REC. - VITALS	x	MENTAL HEALTH	x
x	CLINICAL INFO RESOURCE NETWORK	x	GENERIC CODE SHEET		MICOM	
	CLINICAL MONITORING SYSTEM		GRECC		MINIMAL PATIENT DATASET	x
x	CLINICAL PROCEDURES	x	HEALTH DATA & INFORMATICS	x	MYHEALTHEVET	x
X	CLINICAL REMINDERS	x	HEALTH LEVEL SEVEN		Missing Patient Reg (Original) A4EL	X
X	CMOP	x	HEALTH SUMMARY	x	NATIONAL DRUG FILE	x
x	CONSULT/REQUEST TRACKING	x	HINQ		NATIONAL LABORATORY TEST	x
x	CONTROLLED SUBSTANCES		HOSPITAL BASED HOME CARE	x	NDBI	x
X	CPT/HCPCS CODES	x	ICR - IMMUNOLOGY CASE REGISTRY	x	NETWORK HEALTH EXCHANGE	x
	CREDENTIALS TRACKING	x	IFCAP	x	NOIS	
x	DENTAL	x	IMAGING	x	NURSING SERVICE	x
x	DIETETICS	x	INCIDENT REPORTING	x	OCCURRENCE SCREEN	x
x	DISCHARGE SUMMARY	x	INCOME VERIFICATION MATCH	x	ONCOLOGY	
x	DRG GROUPER	x	INCOMPLETE RECORDS TRACKING	x	ORDER ENTRY/RESULTS REPORTING	x

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Minor app #1

Name	Description	Comments

Is PII collected by this min or application?

Does this minor application store PII?

If yes, where?

Who has access to this data?

Minor app #2

Name	Description	Comments

Is PII collected by this min or application?

Does this minor application store PII?

If yes, where?

Who has access to this data?

Minor app #3

Name	Description	Comments

Is PII collected by this min or application?

Does this minor application store PII?

If yes, where?

Who has access to this data?

OUTPATIENT PHARMACY	x	SOCIAL WORK
PAID	x	SPINAL CORD DYSFUNCTION
PATCH MODULE	x	SURGERY
PATIENT DATA EXCHANGE		SURVEY GENERATOR
PATIENT FEEDBACK	x	TEXT INTEGRATION UTILITIES
PATIENT REPRESENTATIVE	x	TOOLKIT
PCE PATIENT CARE ENCOUNTER		UNWINDER
PCE PATIENT/IHS SUBSET		UTILIZATION MANAGEMENT ROLLUP
PHARMACY BENEFITS MANAGEMENT	x	UTILIZATION REVIEW
PHARMACY DATA MANAGEMENT	x	VA CERTIFIED COMPONENTS - DSSI
PHARMACY NATIONAL DATABASE	x	VA FILEMAN
PHARMACY PRESCRIPTION PRACTICE	x	VBECS
POLICE & SECURITY	x	VDEF
PROBLEM LIST	x	VENDOR - DOCUMENT STORAGE SYS
PROGRESS NOTES		VHS&RA ADP TRACKING SYSTEM
PROSTHETICS		VISIT TRACKING
QUALITY ASSURANCE INTEGRATION	x	VISTALINK
QUALITY IMPROVEMENT CHECKLIST	x	VISTALINK SECURITY
QUASAR	x	VISUAL IMPAIRMENT SERVICE TEAM ANRV
RADIOLOGY/NUCLEAR MEDICINE	x	VOLUNTARY TIMEKEEPING
RECORD TRACKING	x	VOLUNTARY TIMEKEEPING NATIONAL
REGISTRATION	x	WOMEN'S HEALTH
RELEASE OF INFORMATION - DSSI		CARE TRACKER
REMOTE ORDER/ENTRY SYSTEM		
RPC BROKER		
RUN TIME LIBRARY		
SAGG		
SCHEDULING		
SECURITY SUITE UTILITY PACK		
SHIFT CHANGE HANDOFF TOOL		

(FY 2010) PIA: Minor Applications

Add any information concerning minor applications that may be associated with your system. Please indicate the name of the minor application, a brief description, and any comments you may wish to include. If you have more than 3 minor applications please copy then below sections as many times as needed.

Minor app #1

Name

Description

Comments

□ Is PII collected by this min or application?

□ Does this minor application store PII?

If yes, where?

Who has access to this data?

Minor app #2

Name

Description

Comments

□ Is PII collected by this min or application?

□ Does this minor application store PII?

If yes, where?

Who has access to this data?

Minor app #3

Name

Description

Comments

□ Is PII collected by this min or application?

□ Does this minor application store PII?

If yes, where?

Who has access to this data?

(FY 2010) PIA: Final Signatures

Facility Name: Huntington VAMC

Title:	Name:	Phone:	Email:
Privacy Officer:	Diana Bowen	304-429-6755 ext. 3609	diana.bowen@va.gov
BOWEN, DIANA	Digitally signed by: BOWEN, DIANA DN: CN = BOWEN, DIANA O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff Date: 2010.01.22 07:49:48 -05'00'		
Information Security Officer:	Vickie Hisman	304-429-6755 ext. 3234	vickie.hisman@va.gov
VICKIE HISMAN	Digitally signed by: VICKIE HISMAN DN: CN = VICKIE HISMAN O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff Date: 2010.01.22 07:59:42 -05'00'		
Chief Information Officer:	Mary Curry	304-429-6755 ext. 2298	mary.curry@va.gov
Mary M. Curry	Digitally signed by: MARY M CURRY 141662 DN: CN = MARY M CURRY 141662 O = internal OU = people Date: 2010.01.22 14:32:15 -05'00'		
Person Completing Document:	Vickie Hisman	0	0
VICKIE HISMAN	Digitally signed by: VICKIE HISMAN DN: CN = VICKIE HISMAN O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff Date: 2010.01.22 08:00:24 -05'00'		
System / Application / Program Manager:	0	0	0

Date of Report: 12/22/2009

OMB Unique Project Identifier 029-00-01-11-01-1180-0

Project Name	Region 3 > VHA > VISN 9> Huntington VAMC > VISTA-VMS